实验 1.1 Wireshark 软件使用与 ARP 协议分析

一． 实验目的

学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包；掌握以太网 MAC 帧的基本结构，掌握 ARP 协议的特点及工作过程。

二． 实验内容

使用 Wireshark 抓取局域网的数据包并进行分析：

1. **学习 Wireshark 基本操作：**重点掌握捕获过滤器和显示过滤器。
2. **观察 MAC 地址：**了解 MAC 地址的组成，辨识 MAC 地址类型。
3. **分析以太网帧结构：**观察以太网帧的首部和尾部，了解数据封装成帧的原理。
4. **分析 ARP 协议：**抓取 ARP 请求和应答报文，分析其工作过程。

三． 实验原理

3.1 Wireshark 简介

Wireshark 软件是目前全球使用最广泛的开源网络数据包分析工具（前身为 Ethereal），由 Gerald Combs 编写并于 1988 年获开源许可发布。网络数据包分析是指进入网络通信系统、捕获和解码网络上实时传输数据以及搜集统计信息的过程。通过 Wireshark 对网络数据进行分析，我们能够了解网络是如何运行的、数据包是如何被转发的、应用是如何被访问的；能够分析各层网络协议的性能、掌握通信主体的运行情况，确认带宽分配和时延大小、查看应用的快慢并改进优化，识别网络中存在的攻击或恶意行为、解决网络异常和故障。Wireshark 可以在 Windows、Linux 和 macOS 操作系统中运行，具备友好的图形界面、丰富的统计及图表分析功能。

3.2 以太网 MAC 帧格式

本实验基于使用最广泛的有线局域网（以太网 Ethernet II），以太网的帧结构如表1.1–1所示。其中，MAC 地址（Media Access Control Address，媒体存取控制位址）或

称物理地址（Physical Address），用于在网络中标识网卡。MAC 地址的长度为 48 位 (6 个字节)，通常表示为 12 个 16 进制数，如：00-16-EA-AE-3C-40。其中前 3 个字节的 16 进制数 00-16-EA 代表网络硬件制造商的编号、即组织唯一标志符 (OUI)，它由 IEEE 分配；而后 3 个字节的 16 进制数 AE-3C-40 代表该制造商所生产的某个网络产品 (如网卡) 的系列号。

表 1.1–1 以太网帧格式

前导字符	目的 MAC 地址	源 MAC 地址	类型	IP 数据报	帧校验
8 字节	6 字节	6 字节	2 字节	46-1500 字节	4 字节

3.3 ARP 协议及数据报格式

地址解析协议（Address Resolution Protocol，ARP），主要作用是将 IP 地址解析为 MAC 地址。当某主机或网络设备要发送数据给目标主机时，必须知道对方的网络层地址（即 IP 地址），而且在数据链路层封装成帧时，还必须有目标主机（或下一跳路由器）的 MAC 地址。本实验重点观察最简单的情形：同一个网段内，主机 A 要向主机 B 发送信息时，ARP 解析的过程（主机 A 和 B 不在同一网段的情况请参阅课本相关内容）。具体如下：

1. 主机 A 首先查看自己的 ARP 表。如果找到了主机 B 的 MAC 地址，则利用这个地址对 IP 数据报进行帧封装，并将数据报发送给主机 B。
2. 如果主机 A 在 ARP 表中找不到主机 B 的 MAC 地址，则以广播方式发送一个 ARP 请求报文。ARP 请求报文中的发送端 IP 地址和发送端 MAC 地址为主机 A 的 IP 地址和 MAC 地址，目标 IP 地址和目标 MAC 地址为主机 B 的 IP 地址和全 0 的 MAC 地址。由于 ARP 请求报文以广播方式发送，该网段上的所有主机都可以接收到该请求，但只有被请求的主机 B 会对该请求进行处理。
3. 主机 B 比较自己的 IP 地址和 ARP 请求报文中的目标 IP 地址，当两者相同时进行如下处理：将 ARP 请求报文中的发送端（即主机 A）的 IP 地址和 MAC 地址存入自己的 ARP 表中。然后以单播方式发送 ARP 响应报文给主机 A，其中包含了自己的 MAC 地址。

4. 主机 A 收到 ARP 响应报文后，将主机 B 的 MAC 地址加入到自己的 ARP 表中以用于后续报文的转发，同时将 IP 数据报进行封装后发送出去。

ARP 报文结构如图1.1–1所示，ARP 报文总长度为 28 字节，MAC 地址长度为 6 字节，IP 地址长度为 4 字节。每个字段的含义如下：

- **硬件类型：**指明了发送方想知道的硬件接口类型，以太网的值为 1。
- **协议类型：**表示要映射的协议地址类型。IP 地址的类型值为 0x0800。
- **硬件地址长度和协议地址长度：**分别指出硬件地址和协议地址的长度，以字节为单位。在以太网中，它们的值分别为 6 和 4。
- **操作码（op）：**用来表示这个报文的类型，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4。

图 1.1–1 ARP 报文结构示意图

3.4 实验方法及手段

使用 Wireshark 软件在有线局域网中捕捉相关网络操作的数据包，运用观察对比、计算验证、分析统计等方法，掌握以太网 MAC 帧和 IP 数据报的结构以及 ARP 协议的工作原理。

四． 实验条件

- PC 机一台，连入局域网；

- Wireshark 软件，建议 3.0 以上版本。

五． 实验步骤

5.1 WireShark 基本使用

1. 通过 Wireshark 官网下载最新版软件，按默认选项安装。
2. 运行 Wireshark 软件，程序界面会显示当前的网络接口列表，双击要观察的网络接口，开始捕捉数据包，Wireshark 软件选择网络接口的界面如图1.1–2所示。

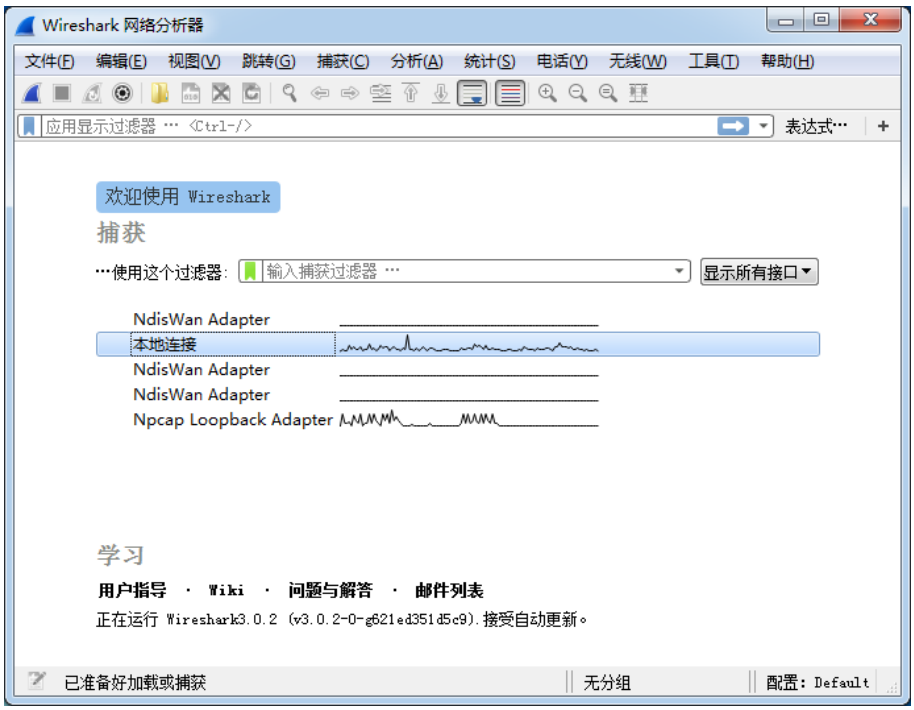

图 1.1–2 Wireshark 软件启动界面

3. 点击工具栏上的红色方块按钮停止捕捉。
4. 菜单、工具栏、状态栏和主窗口如图1.1–3所示，可以根据需要通过菜单“视图”以及“编辑/首选项/外观”的相关选项对基本设置进行更改。例如图1.1–4中的语言、字体缩放、颜色、布局等项目。
5. 使用“显示过滤器”可以方便地从捕获的数据包中筛选出要观察的数据包。显示过滤器支持若干的过滤选项：源 MAC、目的 MAC、源 IP、目的 IP、TCP/UDP 传输协议、应用层协议（HTTP, DHCP）、源端口 Port、目的端口 Port 等。在显示

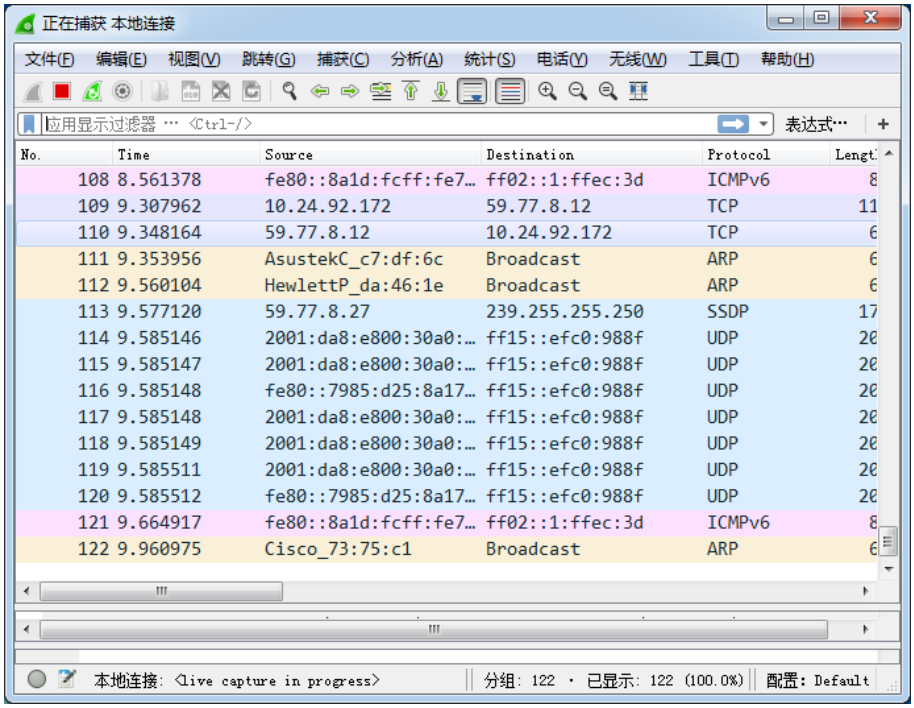

图 1.1–3 Wireshark 主窗口界面

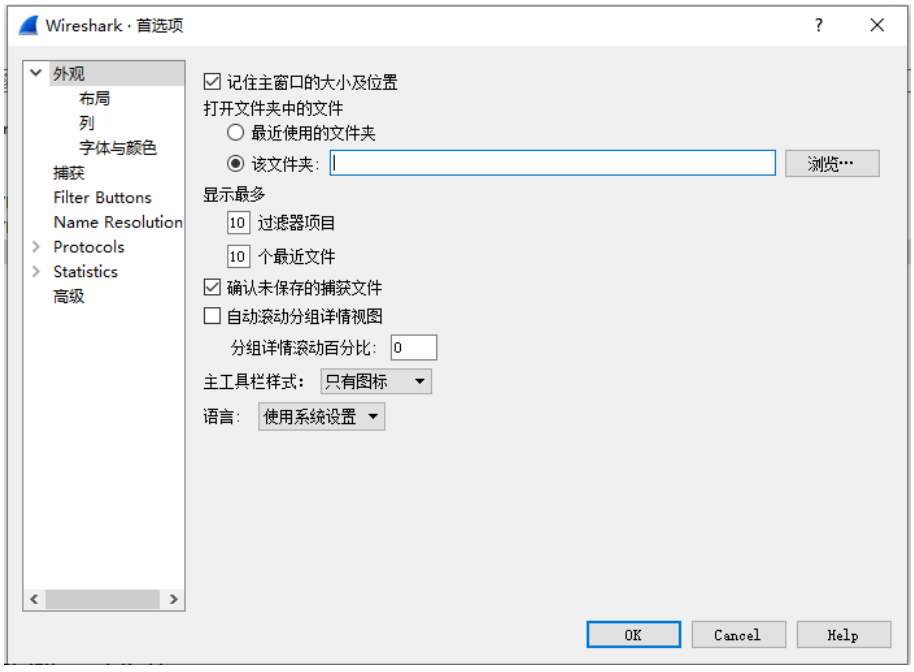

图 1.1–4 Wireshark 的设置界面

过滤器栏中输入过滤表达式（更详细的显示过滤语法可以查看 WireShark 的官方文档[1]），例如下面的命令：

- `arp` //显示 arp 协议报文，例如图1.1--5
- `ip.src == a.b.c.d && icmp` //显示源地址为 a.b.c.d 的 icmp 报文

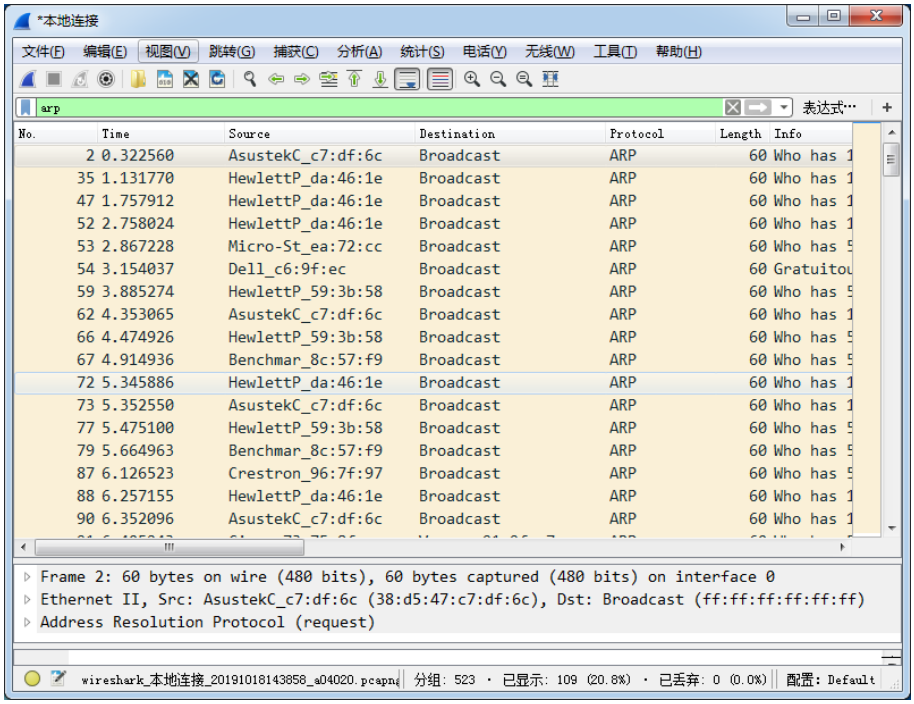

图 1.1–5 显示过滤规则的示例

6. 通过主菜单“文件”/“导出特定分组”（如图1.1–6），可以保存捕获的网络数据（也可以先选中某些包，只保存部分数据）。
7. 如果只想捕捉特定的数据包，可以使用菜单“捕获”/“捕获过滤器”选定想要的类型（如图1.1–7）。例如，选择“IPv4 only”，Wireshark 只抓取 ipv4 类型的数据包。Wireshark 过滤器官方文档提供了更加全面详细的语法和常用示例[2]。
8. Wireshark 还提供了丰富的统计功能供用户选用，如图1.1–8。更多文档可以查询 Wireshark 使用帮助[3]。

[1] WireShark 显示过滤器语法
[2] WireShark 常用过滤器语法
[3] WireShark 学习手册

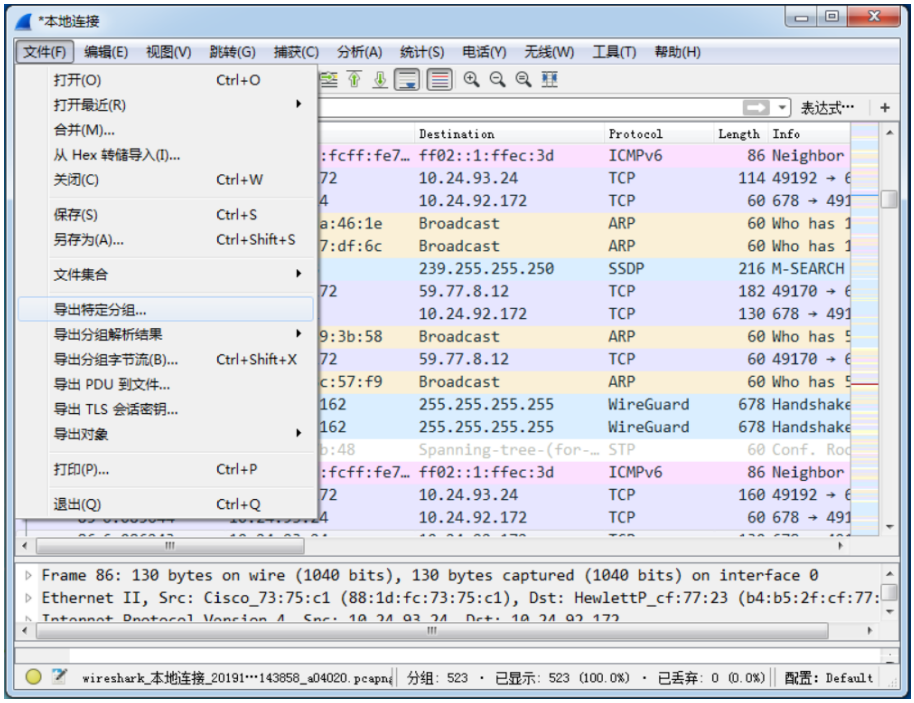

图 1.1–6 操作主菜单保存数据文件

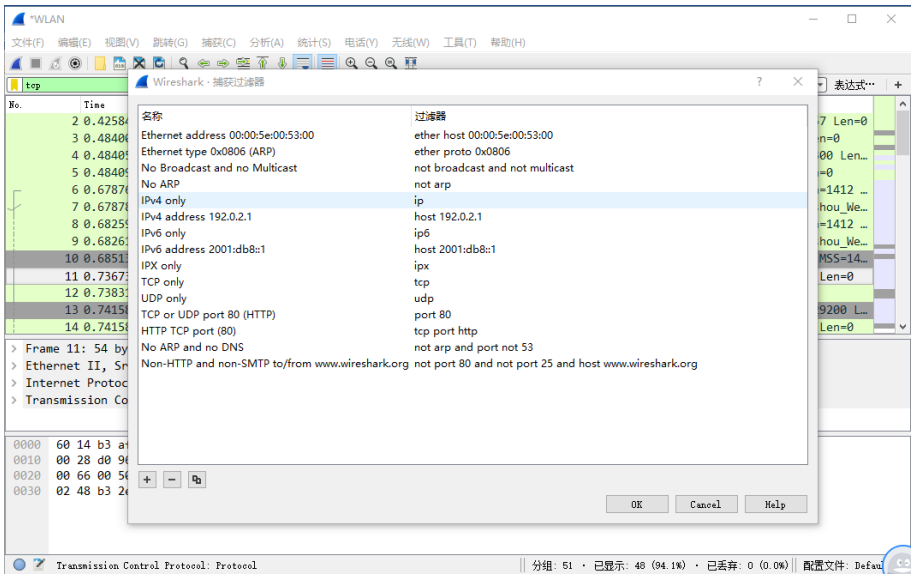

图 1.1–7 选中特定的捕获类型

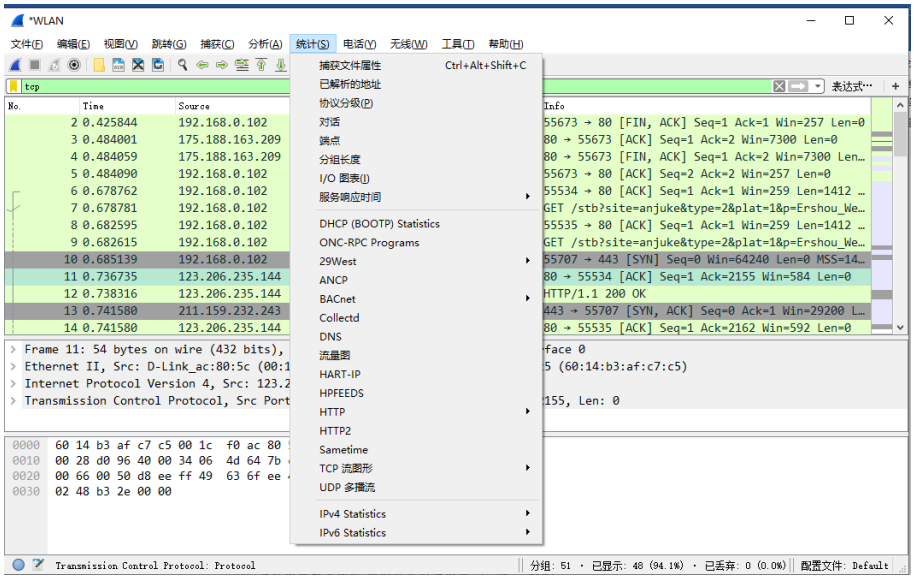

图 1.1–8 统计功能

5.2 观察 MAC 地址

启动 Wireshark 捕捉数据包，在命令行窗口分别 ping 网关和 ping 同网段的一台主机，分析本机发出的数据包。重点观察以太网帧的 Destination 和 Source 的 MAC 地址，辨识 MAC 地址类型，解读 OUI 信息、I/G 和 G/L 位。

5.3 分析以太网的帧结构

选择其中一个数据包，点击 Ethernet II 展开（图1.1–9），查看 MAC 帧的各个字段。

5.4 ARP 协议分析

1. 使用 `arp -d` 命令（其语法见图1.1–10），清空本机的 ARP 缓存，开启 Wireshark，ping 本机的同网段地址，在显示过滤器条框中输入“`arp`”，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。
2. 使用 `arp -d` 命令，清空本机的 ARP 缓存。开启 Wireshark，ping 与本机网段不同的 IP 地址或域名，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

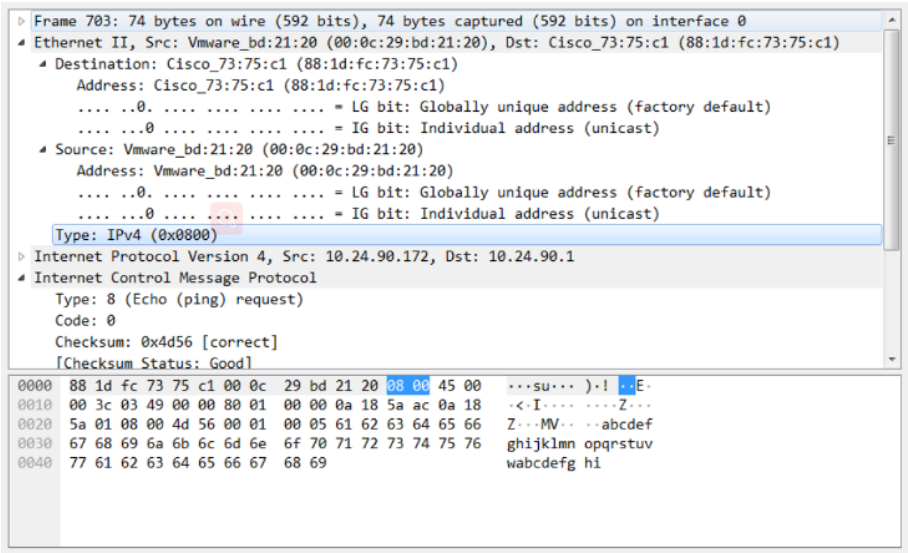

图 1.1–9 以太网帧结构展开界面

```
arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]]
    [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]

  -a 显示所有接口/特定接口的当前 ARP 缓存表
  -g 同 -a
  -d 删除所有/指定的 IP 地址项
  -s 在 ARP 缓存中添加对应 InetAddr 地址的 EtherAddr 地址静态项
```

图 1.1–10 arp 命令语法及参数

六. 考核方法

本次实验需提交一份实验报告以及相关的数据报文保存文件。报告内容应包含以下内容，相关的分析解释都需要截图证明，并与提交的 Wireshark 抓包数据文件相吻合。

1. 以太网帧格式分析：MAC 地址类型、头部信息、长度等信息。
2. 结合捕捉的网络数据，分析 ARP 数据包，描述 ARP 协议工作过程（请求/响应）。
3. 记录自己在本次实验中所遇到的问题，以心得感悟。如果遇到异常情况，或者无法完成任务时，也请分析错误产生的原因。

实验报告要求至少包含以下几个部分：

- 姓名，学号
- 数据报文的相关截图
- 相关分析和结论
- 相关问题和解决方法

源码和实验报告打包按照（计算机网络第一次作业_姓名_学号）的命名格式发送到1255767846@qq.com，截止时间为11月6日24点。

实验报告以word或pdf格式均可，推荐使用latex排版。